

**Notice of Allowability**

Application No.

09/773,716

Examiner

Carl Colin

Applicant(s)

CHATANI ET AL.

Art Unit

2136

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Correspondence received and Interview held on 9/28/2006.
2. ☒ The allowed claim(s) is/are 88-97 and 99-109.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |  |
|--|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 5. <input type="checkbox"/> Notice of Informal Patent Application  |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 6. <input checked="" type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date <u>20060929</u> . |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____    | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment  |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance                         |
|  | 9. <input type="checkbox"/> Other _____  |

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
9,29,06

## DETAILED ACTION

### EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Albert Penilla and correspondence received via E-mail on September 28, 2006 (see attached).

The application has been amended as follows:

**Claim 98** is cancelled.

**Claim 88**, steps (e) and (f) are amended as shown below:

(e) obtaining a title private key that is asymmetrically double encrypted by the server computer using the console public key and the user private key, wherein use of the console public key created at the user computer defining a first layer of encryption, use of the user private key created at the server computer defining a second layer of encryption, the title private key and the title public key defining a title key pair created at the server computer; and

(f) decrypting the title public key encrypted software product using the title private key;

wherein the decrypting the title public key encrypted software product provides access to the software product.

**Claim 94**, steps (e) and (f) are amended as shown below:

(e) retrieving a title private key based on the title ID received, the title private key being double encrypted by the server computer using the console public key and the user private key, ~~use of~~ wherein the console public key created at the user computer defining a first layer of encryption, ~~use of~~ the user private key created at the server computer defining a second layer of encryption, the title private key and the title public key defining a title key pair created at the server computer; and

(f) forwarding the double encrypted title private key to the user computer so that the user computer can use the title private key to decrypt the software product encrypted by using the title public key;

wherein the decrypting the software product provides access to the software product.

**Claim 100**, steps (f) and (g) are amended as shown below:

(f) program instructions for obtaining a title private key that is asymmetrically double encrypted by the server computer using the console public key and the user private key, wherein ~~use of~~ the console public key created at the user computer defining a first layer of encryption, ~~use of~~ the user private key created at the server computer

Art Unit: 2136

defining a second layer of encryption, the title private key and the title public key

defining a title key pair created at the server computer; and

(g) program instructions for decrypting the title public key encrypted software product using the title private key;

wherein the decrypting the title public key encrypted software product provides access to the software product.

**Claim 106**, steps (f), (g), and (h) are amended as shown below:

(f) program instructions for retrieving a title private key based on the title ID received, the title private key and the title public key defining a title key pair created at the server computer;

(g) program instructions for double encrypting the title private key using the console public key and the user private key, ~~use of~~ wherein the console public key created at the user computer defining a first layer of encryption, ~~use of~~ the user private key created at the server computer defining a second layer of encryption; and

(h) program instructions for forwarding the double encrypted title private key to the user computer so that the user computer can use the title private key to decrypt the software product encrypted by using the title public key;

wherein the decrypting the software product provides access to the software product.

*Reasons for Allowance*

2. The following is an examiner's statement of reasons for allowance: The prior art of record US Patent 6,470,085 to Uranaka et al teaches a method and system for permitting an authentic user to play a desired one of application contained in distributed application package which is achieved in the following way the key is obtained in a user public key-encrypted form from a DVD or online from a server, the user public key-encrypted key is decrypted with a user key stored in an IC card into a decrypted key and the encrypted charged information is decrypted with the decrypted key and is played or executed. Bruce Schneier (Non-Patent Literature) discloses well-known cryptographic processes with respect to asymmetric and symmetric cryptography. The prior art of record US Patent 6,260,141 to Park teaches software license control system based on software registration servers including creating secret/public key pair for a user connecting to a server and receiving the server public key, registering a user and receiving an ID file that includes user information encrypted by the user public key and digitally signed by the server secret key; registering a user computer hardware and receiving a license file that includes hardware information encrypted by user public key and digitally signed by the server secret key and registering and receiving an updated license file which now includes the registered software product information and the computer information. The prior arts of record, however, fail to teach singly or in combination: "A method for enabling access to a software product, communication to enable the access to the software product being between a user computer and a server computer, the user computer executing program instructions to enable the method, and orderly processing of operations from (a) to (f), the method comprising: (a) initiating access to the server computer, the initiating causing creation, at the server computer, of

Art Unit: 2136

a user public key and a user private key defining a user key pair at the server computer, the server computer communicating the user public key to the user computer, and the user key pair being generated using information from a specific user; (b) creating at the user computer, a console public key and a console private key defining a console key pair; (c) sending the console public key to the server computer, the console public key being encrypted using the user public key; (d) forwarding a title ID to the server computer to enable access to the software product that is encrypted using a title public key, the title ID being encrypted using the user public key; (e) obtaining a title private key that is asymmetrically double encrypted by the server computer using the console public key and the user private key, wherein the console public key created at the user computer defining a first layer of encryption, the user private key created at the server computer defining a second layer of encryption, the title private key and the title public key defining a title key pair created at the server computer; and (f) decrypting the title public key encrypted software product using the title private key; wherein the decrypting the title public key encrypted software product provides access to the software product” as recited in independent claim 88. Independent claims 94, 100, and 106 recite similar limitations. Consequently, claims 88, 94, 100, and 106 are allowable over the prior arts of record. Claims 89-93, 95-97, 99, 101-105, 107-109 are directly or indirectly dependent upon claims 88, 94, 100, and 106, and therefore are also allowable over the prior arts of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Art Unit: 2136

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin  
Patent Examiner  
September 29, 2006

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
9/29/06